JAPANESE PATENT OFFICE

EP0520709
for
JP5274266

PATENT ABSTRACTS OF JAPAN

A method for providing a security facility for remote systems management.

Publication date: 1992-12-30
Inventor(s): GRIFFIN DAVID MICHAEL (US); TALLMAN OWEN HAROLD (US); JOHNSON BRAD C (US); SEALY DEXTER (US); SHELHAMER JAMES (US); SUDAMA RAM (US)
Applicant(s):: DIGITAL EQUIPMENT CORP (US)
Application Number: EP19920305673 19920619
Priority Number(s): US19910722879 19910628
IPC Classification: G06F1/00
EC Classification: G06F12/14D3T

Abstract

This invention consists of a method for providing security for distributing management operations among components of a computer network using a network of mutually trusting, mutually authenticating management services to dispatch operations to selected host systems. Mutual authentication and trust are established on every transmission link from a point of submission to a designated management server which invokes a service provider to perform management operations on a selected host.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－274266

(43)公開日　平成５年(1993)10月22日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ａ	7459－5L		
	1/00	３７０　Ｅ	7927－5B		
	12/00	５３７　Ｄ	7232－5B		
	13/00	３５１　Ｚ	7368－5B		
	15/16	３７０　Ｚ	9190－5L		

審査請求　未請求　請求項の数11(全 14 頁)

(21)出願番号　特願平4－169622

(22)出願日　平成４年(1992)６月26日

(31)優先権主張番号　０７／７２２８７９

(32)優先日　1991年６月28日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590002873
ディジタル　イクイプメント　コーポレイション
アメリカ合衆国　マサチューセッツ州　01754メイナード　メイン　ストリート　146

(72)発明者　ラム　サダマ
アメリカ合衆国　マサチューセッツ州　01749ハドソン　レイク　ショア　ドライヴ　14

(74)代理人　弁理士　中村　稔　（外６名）

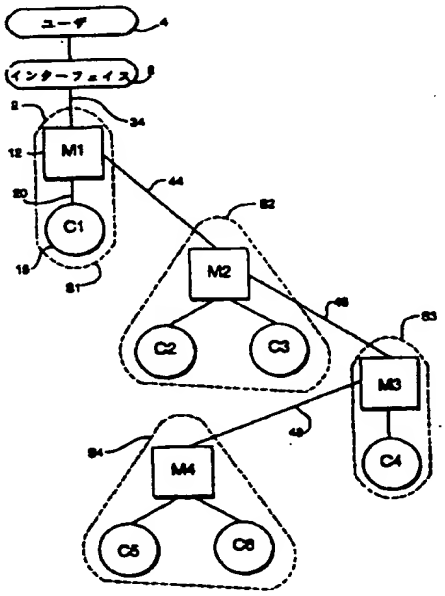
最終頁に続く

(54)【発明の名称】　遠隔システム管理のための機密保護機能を提供するための方法

(57)【要約】

【目的】　本発明は、ネットワーク化されたデータ処理システムための従来技術による機密保護機能の問題を克服し、委任の半永久的な形を利用することによって安全なネットワーク環境を保全する。

【構成】　この発明は、選択されたホストシステムにオペレーションを送信する管理サービスを相互に認証し、相互に信頼するネットワークを使用して、コンピュータネットワークの構成要素間に管理オペレーションを分配するための、機密保護を提供する方法から成る。選択されたホスト上で管理オペレーションを実行するために、サービス供給者を呼び出す指定の管理サーバへ、実行依頼点からすべての伝送リンク上に、相互の認証および信頼が確立される。



1

【特許請求の範囲】

【請求項１】　データ処理ネットワークのための機密保護を提供する方法であって、前記ネットワークが（ｉ）実行すべきオペレーションを通信するために、伝送によって接続される複数の処理サーバと（ii）一つの信頼関係が通信するためにリンクされた処理サーバ間に存在するということを確認するための複数の信頼関係のデータベースとを有するようになっている機密保護提供方法において、

信頼関係のデータベースから実行すべきオペレーションを受信するための信頼された処理サーバの身元を検索し、

身元確認され信頼された受信処理サーバへの処理サーバの１つからの実行すべきオペレーションを送信し、そして、

信頼された受信処理サーバによって送信処理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【請求項２】　データ処理ネットワークのための機密保護を提供する方法であって、

前記ネットワークがオペレーションに記述されている機能を実行するように指定されたホストに連結されているユーザおよび最終管理サーバからの、オペレーションを実行せよという実行依頼点を提供するための少なくとも１の発信管理サーバを持ち、またオペレーションに記述された機能を実行するように指定されたホストの身元確認を行ない、かつ、発信管理サーバから最終管理サーバまでのパスを形成するリンクのリストを含むデータベースを持つようなシステムにおける機密保護提供方法において、

発信管理サーバによる実行すべきオペレーションを受信し、

最終管理サーバの身元を確認し、

発信管理サーバから最終管理サーバまでの信頼されたパスの身元を確認し、

データベース内に含まれている諸関係と一致する、発信管理サーバと最終管理サーバ間のパスに対するオペレーションを転送し、また、

最終管理サーバによる発信管理サーバとの信頼関係の存在を確認するというステップを含むことを特徴とする前記方法。

【請求項３】　請求項２に記載の方法において、発信管理サーバから最終管理サーバまでのパス上の各リンクが信頼されたリンクであり、そのリンクに対しする信頼関係が各々の送受信する管理サーバ間に存在し、

信頼関係のデータベースから実行すべきオペレーションを受信するための信頼された処理サーバの身元を検索し、

身元確認された信頼された受信処理サーバへの処理サーバの１つからの実行すべきオペレーションを送信し、そして、

2

信頼された受信処理サーバによって、送信処理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【請求項４】　請求項３に記載の方法において、最終管理サーバとの信頼関係の存在をホストによって確認するステップをさらに含み、最終管理サーバを認証するステップをホストによってさらに含むことを特徴とする前記方法。

【請求項５】　データ処理ネットワークのための機密保護を提供する方法であって、前記ネットワークが、ユーザおよび最終管理サーバから、オペレーションに対する実行すべき実行依頼点を提供するための少なくとも１つの発信管理サーバと、オペレーション中に記述されている機能を実行するように指定されたホストに最終管理サーバが連結されており、オペレーションに記述されている機能を実行するように指定されているホストの身元を確認し、かつ、発信管理サーバから最終管理サーバまでの信頼されたパスを形成するリンクのリストを含んでいるデータベースとを持つようなシステムにおける機密保護を提供する方法において、

発信管理サーバによって実行すべきオペレーションを受信し、

最終管理サーバの身元を確認し、

発信管理サーバから最終管理サーバまでの信頼されたパスの身元を確認し、

発信管理サーバによって最終管理サーバの身元を検索し、

データベース内に含まれている諸関係と一致する、発信管理サーバと最終管理サーバ間のパスに対するオペレーションを転送し、そして、

最終管理サーバによって発信管理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【請求項６】　請求項５に記載の方法に従って、データ処理ネットワークに機密保護を提供する方法において、

送信中間管理サーバによって最終管理サーバの身元を検索し、

データベース内に含まれている信頼関係と一致する、送信中間管理サーバ間の信頼されたリンクに対するオペレーションの最終管理サーバへ転送し、そして最終管理サーバによって送信中間管理サーバとの信頼関係の存在を確認することをふくむことを特徴とする前記方法。

【請求項７】　請求項６に記載の方法において、前記の少なくとも１つの通信上連結された中間管理サーバが通信上連結された少なくとも２つの中間管理サーバを含み、また、前記方法がさらに送信中間管理サーバによる受信中間管理サーバの身元を検索し、

データベース内に含まれている諸関係と一致する、送信中間処理サーバと受信中間処理サーバ間の信頼されたリ

ンク上のオペレーションを転送し、そして、
受信中間処理サーバによる送信中間処理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【請求項８】　請求項６に記載の方法において、送信管理サーバと信頼された受信管理サーバとの間で相互を認証するステップをさらに含み、また、ホストが実行すべき機能を指定するオペレーションの実行を依頼するユーザの許可をホストが確認するステップをさらに含むことを特徴とする前記方法。

【請求項９】　請求項８に記載の方法において、最終管理サーバとの信頼関係の存在をホストが確認するステップをさらに含み、最終管理サーバをホストが認証するステップをさらに含むことを特徴とする前記方法。

【請求項１０】　データ処理ネットワーク上の複数のホストを含んでいる複合オペレーションを実行するための機密保護を提供するための方法であって、前記ネットワークが実行すべき複合オペレーションの実行依頼点をユーザから提供するための少なくとも１つの発信管理サーバと、複合オペレーションに記述された機能を実行する第１ホストのための複合オペレーションを受信する調製管理サーバと、第２ホストのための最終管理サーバ、および複合オペレーションに記述されている機能を実行するように指定された第１ホストおよび第１ホストから送られるオペレーションを実行する第２ホストの身元を確認し、発信管理サーバから調製管理サーバまでの、並びに、調製管理サーバから最終管理サーバまでのパスを形成するリンクのリストを含んでいるデータベースを持っているシステムにおける機密保護を提供するためのホストにおいて、
発信管理サーバによる実行すべき複合管理オペレーションを受信し、
調製管理サーバの身元を確認し、
発信管理サーバから調製管理サーバまでの信頼されたパスの身元を確認し、
発信管理サーバと調製管理サーバ間のパスに対する複合オペレーションを転送し、
調製管理サーバによる発信管理サーバとの信頼関係の存在を確認し、
調製管理オペレーションから第１ホストまでの複合オペレーションを転送し、
第２ホストが実行すべきコマンドを第１ホストから実行依頼し、
最終管理サーバの身元を確認し、
調製管理サーバから最終管理サーバまでの第２の信頼されたパスの身元を確認し、
データベース内に含まれている諸関係と一致する、調製管理サーバと最終管理サーバとの間の第２パスへのコマンドを転送し、そして最終管理サーバによる調製管理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【請求項１１】　請求項１０に記載の方法において、発信管理サーバから調製管理サーバまでのパスおよび調製管理サーバから最終管理サーバまでのパス上のリンクが、信頼されたリンクであって、リンクに対する信頼関係が各々の信頼されたリンク上の各送受信管理サーバ間に存在し、
実行すべきオペレーションを信頼関係のデータベースから受信するための信頼された管理サーバの身元を検索し、
管理サーバの１つから身元確認された信頼された受信管理サーバへ、実行すべきオペレーションを送信し、そして信頼された受信管理サーバによって、送信管理サーバとの信頼関係の存在を確認するステップを含むことを特徴とする前記方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はネットワーク化されたデータ処理システムに関するものであり、特に、遠隔システム処理（ＲＳＭ）用の機密保護機能を提供する方法に関する。ＲＳＭは、ネットワーク上の実行システムおよび適用業務管理機能から成る。例えば、アカウントの作成がシステム管理機能である場合、ネットワーク上でのシステムでのアカウントの作成は遠隔のシステム管理機能である。

【０００２】

【従来の技術】ネットワーク化されたデータ処理システムは、集中データ処理システムに対していくつかの利点を提供する。第１に、分散処理システムは、複数の利用可能なネットワーク処理資源（“ネットワーク資源”）へ、サービス要求を割り当てることによって、システムユーザによる情報処理要求を効率的に実行するための手段を提供する。ネットワークの相互に連結したノードに存在するオペレーティングシステムは、ネットワーク中のノードと呼ばれる多くの記憶場所の間のネットワーク資源およびデータによって実行される機能の記述を持つオペレーションパケットの転送によって、容易に利用可能な資源へ作業量を分散するために協力する。以下“処理サーバ”と呼ぶことにするネットワーク・ノード上を走るあるプロセスは、別個の処理サーバのコントロールの下で走る、ネットワークの別の局所的なシステム間のネットワーク資源によって機能を実行するために、データおよび要求のルーティングを制御する。典型的に述べるならば、局所的なシステム（すなわち単一の処理サーバのコントロール範囲内の）上で作動するプロセスは、ネットワークプロトコルとは独立して別個に実行される。これらのプロセスは局所的なデータを自由に操作することができ、局所的に決定することができる。しかしながら、プロセスがネットワーク上で情報を交換する場合、それらは互いと、ネットワーク処理サーバのコント

ロールの下で通信する。

【０００３】処理サーバは、ネットワークのノード間でのネットワーク資源による機能の実行のために、データおよび要求を転送するためのネットワーク通信プロトコルをインプリメントする。これらの処理サーバは送信者ノードからの要求を受信し、ネットワーク要求待ち行列上にこれらの要求を置き、次に、ネットワークオペレーション規則の前もって定義したセットにしたがって指定された転送先コンピュータへ要求を転送する。ネットワーク処理サーバによって強化された規則は、ネットワークの一般的な必要性および特定の必要性に基いて、ネットワーク設計者が決定する。複数のネットワーク処理サーバ間で要求が受け渡される場合、送信ネットワーク処理サーバと受信ネットワーク処理サーバは、一般に、情報通信のために不可欠な規則セットに一致しなければならない。

【０００４】“処理サーバ”とは管理オペレーションに指定された機能を実行する。１セットの関連するプロセスである。管理オペレーションは、処理サービスによって実行されるべき少なくとも１つの機能を指定する情報のパケットおよびその機能の実行を要請する構成要素である。ネットワーク化されたデータ処理システムでは、自動処理サービスは、分散された方法でネットワークの多くの局所的なシステムに提供される。ネットワークのノードのうちの若干は、処理サービス用のホストから成る。そのホストはそれら自身ネットワーク化されたデータ処理システム中で提供されるサービスを使用するアルゴリズム、ワークステーション、パーソナルコンピュータあるいは他のオペレーティングシステムであってもよい。

【０００５】ネットワーク用の普遍的なデータベースは、それらの指定処理サーバへホストをマップする。処理サーバは、データの受取および送出し、並びに、ネットワーク資源要求を調整し、マッピング機能によって各処理サーバとして指定された信頼されたリンクにしたがって指定されたノードへ渡す。管理オペレーションとは、ネットワーク資源によって実行される要求された機能の少なくとも１つの記述、および要求を実行依頼したユーザの身元を含んでいるデータパケットである。処理サーバが管理オペレーションを受信した場合、処理サーバは、処理サーバのコントロールの下で局所サービス供給者に連結されたホストに管理オペレーションを送信してもよいし、あるいは、二者択一的に言えば、処理サーバは、もう一つの処理サーバへオペレーションを転送してもよい。例えば、処理サーバは、あるホストに連結され、特にそのホスト宛にオペレーションを受信するように選定された、もう一つの処理サーバに管理オペレーションを送ってもよい。データベースによって提供されるこのマッピング機能は、開始処理サーバの点から処理オペレーションを転送するために使用される。この開始処理サーバはネットワーク資源による機能を実行するようにというユーザによる要求の実行依頼が、ホストとして指定された処理サーバへ行われる点であり、このホストが順番に、管理オペレーションに記述された処理サーバを処理する。

【０００６】ネットワークでの処理サーバは、局所的なシステムの“機密保護”および局所的なシステム間の通信リンクの“機密保護”を保全する方法で、ネットワーク化されたデータ処理システムにおいて、システム処理（これはネットワーク通信プロトコルを含むものであるが）を実行すべきである。ネットワーク機密保護は、ネットワーク内に含まれているオペレーションあるいはデータへの無許可のアクセスから保護するための手段から伝統的に成っている。このタイプの機密保護は、データ処理ネットワーク内の情報あるいはネットワーク処理資源にアクセスする慎重であると同時に故意でない試みを妨げる。機密保護の別の重要な様相は、データの送信者あるいはネットワーク要求の送信者に与えられる保証で、受取人が送信者によって送信された情報を無許可で使用したり改悪をしないという保証である。“機密保護”とはネットワーク資源へのアクセスを制限することから成るだけでなく、データ要求が、予期した効果を生じる確実なネットワーク資源によって扱われそして／若しくは処理されるという保証を含んでいる。ネットワーク資源とは、例えば、もう一つの別のネットワーク処理サーバ、データ記憶装置システムあるいはデータ処理システムであってもよい。

【０００７】ネットワークにおける機密保護に対する“脅威”とい言葉は、システムの機密保護に対する首尾よくなされた場合の侵犯に帰着するすべての活動を表わすために、ここでは使用されている。脅威がもし無効にされなければ、ユーザが信頼しているネットワークへの情報が、許可なく破壊、変更、複写、送信されるかもしれないし、あるいは処理資源を入手されるかもしれない。ネットワークなしで操作する詐欺者あるいは無許可のプロセスがこれらの脅威を生み出す可能性がある。

【０００８】従来のネットワーク管理機密保護機能は、ネットワーク内のシステムへの脅威のインパクトを減らすために、局所的なオペレーティングシステムおよび局所的なネットワークサービスの中にすでに存在しているメカニズムに依存したものである。そのようなメカニズムは、安全な管理環境を提供するために、パスワード、アクセス管理リストおよび代理を含んでいる。これらの保護ツールは、単一の処理サーバシステム内では安全な環境を十分に提供する。しかしながら、システムが２つ以上の処理サーバおよびデータを含んでいたり、ネットワーク要求を２つ以上の処理サーバ間で送信しなければならない場合、いくつかの問題が提起される。

【０００９】まず第１に、異種混合の管理システム（つまり一貫しないシステム機密保護手段をインプリメント

している局所的なオペレーティングシステムを含んでいるもの）では、ひとたび受信処理サーバが情報の制御を行なえば、ネットワークの局所的なシステム間で送信された情報の同一標準での保護を保証することはできない。受信システムによって利用される機密保護手段は不適当であるかもしれない。あるいは受信処理サーバが順番に非安全なネットワーク資源へ情報を転送するかもしれない。したがって、異種混合の管理システムにおいては、送信者は、受信処理サーバが情報の制御を行なった後に、その情報の秘密性が危険にさらされる可能性という不利益に対して、もう一つの処理サーバによって制御される別のシステム資源に情報を送信する利益を秤に掛けなければならない。

【００１０】次に、従来の機密保護メカニズムの中には、ＲＳＭオペレーション用に設計されたものではないために、ある環境の中で使用された時、完全には安全とはいえないものもある。例えば、２つの処理サーバ間で渡された時、コード化されないパスワードがさえぎられることがある。その場合、制限されたネットワーク資源あるいは情報への無許可のアクセスを得るために、インターセプターはそのパスワードを使うことができる。

【００１１】さらに、各局所的なシステム処理サーバがその局所的なオペレーティングシステムに関連した機密保護手段を変更するプログラミングツールをＲＳＭの領域外に利用する能力を所有していれば、機密保護の侵犯源を突き止めることは困難である。ネットワークの機密保護の弱いリンクをすべて分析するためには、ネットワーク内の各処理サーバの局所的な機密保護手段を調査しなければならない。したがって、これらの従来の技術システムは、局所的な機密保護侵犯の影響を受けやすいばかりでなく、また、機密保護の侵犯源を確認する難しさは、ネットワークのサイズが大きくなるにつれて増大する。

【００１２】したがって、処理サービスに無関係の局所的な機密保護メカニズムを利用する既知のＲＳＭ機密保護機能は、安全なネットワークの保全を望む人にとって、重要な問題を提起するかもしれない。局所的なシステムによって使用される弱い機密保護手段は、ネットワークの他の局所的なシステムによって採用されている機密保護手段に関する情報を持っていない、他の局所的なオペレーティングシステム処理サーバあるいはユーザにとっては明白ではないかもしれない。（侵犯があったかどうかの）診断は各々の局所的なシステムの機密保護手段の知識を要求するので、統一標準でない機密保護規則が種々の局所的なオペレーティングシステムによって使用されている場合、機密保護の侵犯源をシステム中で明らかにすることは面倒である。数個以上のノードでネットワークが成っている場合、これはとても手におえない骨の折れる仕事である。更に、局所的な機密保護手段がネットワーク操作環境の外で局所的なオペレーティングシステムによって変更されるかもしれない場合、機密保護に対する脅威を診断し消去することはさらに面倒である。

【００１３】

【発明が解決しようとする課題】ネットワーク環境で実行されるＲＳＭオペレーションに機密保護を提供するための別のアプローチは、大域ユーザ確認によるものである。一つの例として、キーが特定のプロセスに割当てられる個人のキー暗号サービスが頻繁に使用される。このアプローチは、例えば、限られた数のホストシステムに対して単一の処理サーバを使用する構成が小規模の環境にとって適切であり、また、より大規模なネットワーク環境を含む管理領域が分離されており、ネットワーク許可手続きによる許可無しには変更することができない場合には適切である。しかしながら、たとえこれらの環境下であっても、オペレーションのコントロールが多重システムに及ぶことが許されている管理システムは、コントロールがシステム間で転送される任意の点で攻撃を受けやすいので、機密保護は保証されない。限定のシステム上のプロセスは認証されるかもしれない。すなわち、自身を正直に表してもよい、しかし、許可されたユーザに扮する敵意を持つパーティに利用されるかもしれない。つまり、コントロールの以前の転送危険にさらされたかもしれない。従って、複数の処理サーバが大規模なネットワーク化された計算環境に対して処理サービスを提供する目的で対話する場合、そのようなアプローチは機密保護という問題を十分に処理するものではない。

【００１４】この問題への望ましい解決は、パーティ間で認証された信任状の転送である委任である。ネットワークにまたがる多重システム、プロセスおよびユーザをカバーする、安全でかつ扱いやすい委任方法は、現在存在しない。代りに、従来の委任は、ネットワークの１つのオブジェクト？から次のオブジェクトへ認証された信任状を転送することによるものである。多重システム間を渡された時、これらの信任状は遮断の脅威を受けやすい。

【００１５】

【課題を解決するための手段】本発明は、ネットワーク化されたデータ処理システムための従来技術による機密保護機能の問題を克服し、委任の半永久的な形を利用することによって安全なネットワーク環境を保全する。本発明においては、大域データベースに保全されている信頼関係は、処理サーバ間で許可を委任するという半永久的な形を提供する。したがって、ひとたびユーザが処理サーバに認証されれば、ネットワーク内の１台のホストあるいは１セットのホストに作用してもよいというユーザの許可の下で、ネットワークの処理サーバ間で定義された信頼関係の制限に従って、処理サーバは行動する。ネットワークの処理サーバ間で送信される管理オペレーションのリンク状の保護をインプリメントする、内化さ

れたネットワーク機密保護機能を、本発明による方法は使用する。ネットワークは、送信および受信処理サーバ（つまり、２つの処理サーバ間でその伝送は許可される）間に相互の信頼関係が存在することを要求することによって、処理サーバ間におけるネットワークリンクに対する管理オペレーションの安全な伝送を促進する。機密保護の追加手段として、送信者および受信者は各々相手を認証することを要求される。

【００１６】更に　処理サーバがホストの指定処理サーバであることを確認するために、管理オペレーションを実行依頼し処理サーバを認証し、その要求が信頼されたユーザから発生したものであることを確認するまでは、ホストは、要求された管理オペレーションの実行を保留する。幅広い形式を持つ本発明は、（ｉ）実行されるオペレーションを通信するために、伝送によって接続される複数の処理サーバを有し、また（ii）一つの信頼関係が通信上リンクされた処理サーバ間に存在することを確認するための、複数の信頼関係のデータベースを有する、データ処理ネットワーク用の機密保護を提供するシステムおよび方法にあり、次のステップを含んでいる。すなわち、信頼関係のデータベースから実行されるオペレーションを受信するための信頼された処理サーバの身元検索、身元確認され信頼された受信処理サーバへの処理サーバの１つからの実行されるオペレーションの送信、および、信頼された受信処理サーバによる、送信処理サーバとの信頼関係の存在の確認。ここに説明されるように、各処理サーバによるリンク状の双方向許可チェックの実行は、詐欺師の処理サーバがもう一つの処理サーバに扮することに成功するためには、近隣の処理サーバとの間の信頼関係あるいはあるホストと処理サーバとの関係を知っていなければならないので、ノードをコントロールし、制限されたネットワーク資源に管理オペレーションの実行を依頼する詐欺師の処理サーバの脅威を減少させる。更に、本発明は、ネットワーク機密保護手段をカバーしてコントロールの集中化により、また、処理サーバ間での情報の安全な伝送を提供するための同一標準のセットの規則を提供することによって、ネットワーク機密保護への脅威を検知し削除する困難を減らす。機密保護の集中化は任意の規定の処理サーバからネットワーク資源へのアクセスが、隣接した処理サーバとの以前に確立された信頼関係によって制限されるので局所的なシステムが全体のネットワークの機密保護を単独で危険にさらすことを妨げる。同一標準のセットの規則は、また、システムのさまざまな資源へのアクセス特権を変更するためにネットワーク管理者によって必要とされる知識の量を減らす。

【００１７】以下説明する方法は、複数の処理サーバを有するネットワークに実行依頼されたユーザ要求に応じて作り出される管理オペレーションを実行し、各処理サーバは選択されたホストシステムあるいは他の処理サーバのいずれかと管理オペレーションの受取および送出しを調整する。ユーザは、アクセス時点で認証される。確認と同時に、あるいはすぐその後で、ユーザの身元、および処理サーバによってホストあるいは処理サーバのいずれかに送られる機能の記述を含むユーザの管理オペレーションをネットワークは受信する。ホストシステムは、管理オペレーションに関連したユーザの身元に基いてホストに対する機能の実行を許可するか拒否する。

【００１８】大域データベースは、指定機能を実行するためのホストのリスト、ホストの指定処理サーバおよび処理サーバ間での信頼されたルーティングパスのリストを保全し提供する。管理オペレーションが、発信処理サーバと呼ばれるアクセス点まで連結された処理サーバによって受信された後、指定する処理サーバまでの先定のルートでリンクするプロセスの１つを構成する管理オペレーションあるいは別の管理サーバに記述されている機能を実行するようにデータベースによって指定されているホストと連結している指定処理サーバへ、発信処理サーバは管理オペレーションを転送する。ただし、下記条件を満たすという前提がある。すなわち

１）“信頼関係”が、転送オペレーションに参加する処理サーバ間に存在すること。

【００１９】２）転送オペレーションに参加する処理サーバが相互に認証されていること。もし要求の送信者および受信者が要求の伝送を実行するのに正当なパーティであると、互いによって決定されなければ、ネットワークでの２つの処理サーバ間の伝送は生じない。相互の認証および信頼関係が確立されない場合、管理オペレーションの伝送は送信者あるいは受信者のいずれかによって異常終了させられる。発信処理サーバから転送先処理サーバまでのパスが処理サーバ間で１つ以上の伝送を含んでいる場合、送信者および受信者は、発信処理サーバと指定処理サーバとの間の信頼されたパス上で各々の中間伝送のための前述のテスト条件を満たさなければならない。

【００２０】最終的に、ホストの指定処理サーバがホストにオペレーションの実行要求を提起する場合、ホストが要求を完了する前に、下記条件を満たさなければならない。

１）ホストおよび処理サーバは相互に認証されなければならない。

２）ホストは、この処理サーバを信頼して、その指定処理サーバとして行動させなければならない。

【００２１】３）オペレーションを発信するユーザは、ホストの局所的な許可データに従って、管理オペレーションに述べられている機能に実行を要請する許可を受けなければならない。管理オペレーションは、ユーザの代りにホストから発信されてもよい。これらのオペレーションは以下複合管理オペレーションと呼ばれる。そのような場合、管理オペレーションの実行を依頼するホスト

指定処理サーバは、管理オペレーションを実行するためにターゲットホストへ管理オペレーション（これは最初、発信ホストによって指定処理サーバへ転送される）を転送する。安全なパスは、発信ホストの処理サーバからターゲットホストの処理サーバまで、前述の相互の確認および信頼関係によって促進される。処理サーバがターゲットホストに管理オペレーションを提起する場合、ホストは、管理オペレーションが許可された処理サーバによって示されたことを確認し、管理オペレーションが許可されたホストによって実行依頼されたことを確認する。

【００２２】

【実施例】本発明は、ネットワーク化されたデータ処理システムにおいて使用するための機密保護機能に一般に関する。まもなく説明されるこの発明を具体化するネットワークが、当業者に周知の３つの基本ユーティリティーを所有することが望ましい。第１に、管理オペレーション要求が受信されるユーザー・インターフェースは、ユーザの身元を認証するための確実な方法を所有していなければならない。たとえば、システムは、ネットワーク資源へのアクセスを行なうためにパスワードの実行を依頼することをユーザに要求してもよい。しかしながら、ユーザの身元を認証するための他の任意の有名な方法を本発明を具体化するシステムで採用することができる。第２に、１つの処理サーバによって処理されたプロセスは別のシステムで走るプロセスの確実性を証明するための手段を所有しなければならない。例えば、認証するプロセスのための有名な１つの方法はプロセスを認証するためにいくつかの利用可能なキーベースの暗号システムの１つを利用することである。第３に、オペレーションパケット内で記述された機能を現実に実行する処理サービスは、ネットワーク資源上でユーザ要求を実行するために協力する多様なプロセス間の信頼関係を定義する能力を所有することが望ましい。これは、既定のプロセスへの正当な送信者および既定のプロセスからの受信者をリストする信頼されたサーバテーブルによって遂行されることが望ましい。

【００２３】ネットワークの多くのネットワーク化された計算機システムおよびプロセスに処理サービスを提供する遠隔システム管理（ＲＳＭ）システムに組入れられた時、本発明は特に有用である。第１図は、本発明を具体化するネットワークでの使用に適した局所的なデータ処理システム２の図解表現を示す。第１図は、ネットワーク管理オペレーション要求を生成するユーザ４と管理オペレーションを受信し転送し処理する処理サーバ１２および処理サービス１９を提供するホスト１６との間の関係を示す。局所的なシステム２は、第２図に図解で描写されているようなネットワーク環境において通常作動する。処理サーバ１２は、ネットワークの局所的なシステム２に連結された他のシステムにインタフェースを提

供する。第１図に示される各々の構成要素がコンピュータソフトウェアプログラム、プロセス、手順およびデータパケット内に統合されることを理解するべきである。また、この後提示される実施例の説明は、いかなる特別のシステムハードウェアに限定される意図のものではない。

【００２４】ユーザ４はインタフェース６を通じて、ネットワークとの物理的なユーザの対話に応じて作成されるプロセスである。インタフェース６は、ＲＳＭ領域外にあるが、ユーザ４を認証し、ユーザ４からの管理オペレーションを受信する。管理オペレーションは、ホスト１６によって提供される身元確認された処理サービスによって実行されるべく指定された処理サーバに協同するＲＳＭ処理サーバによって伝送される少なくとも１つの記述を含んでいる。管理オペレーションは、さらにＲＳＭ機能に実行を要請するユーザの身元確認を含んでいる。オペレーションパケットに含まれている本発明に不可欠ではない他の分野は、通常の当業者に周知のものであろう。インタフェース６は、ユーザ処理サーバインタフェース３４によって処理サーバ１２のディスパッチャ２４へ管理オペレーションを伝送する。

【００２５】ディスパッチャ２４は、管理オペレーションを受信し、管理オペレーションのターゲットオブジェクト？（つまり指定処理サービス１９）の指定処理サーバへそれを差し向ける。オペレーションが局所的なシステム２上で実行される場合、管理オペレーションはスケジューラ２６に転送さる。スケジューラ２６は、管理オペレーションをキューに登録、実行し、局所的なシステム２のオペレーション状態を保全する。スケジューラ２６によって実行されるキューイングオペレーションおよびディスパッチャ２４によって実行される一般的な転送オペレーションの両方は共に、オペレーションの受信、その転送先の決定、および適切な受信者へのオペレーションの転送の３つから本質的に成るものであるが、当業者には周知の事柄である。

【００２６】一般に、処理サーバ１２はネットワークの選択されたホスト１６のために１つ以上の処理サービス１９を処理するＲＳＭプロセスである。処理サーバ１２は、処理サービス１９によって実行するべくホスト１６へ管理オペレーションを転送するための適切なコントロールを調整する。処理サーバ１２は、次のようなサービスを実行できる。すなわち、バックアップ、総括的なファイル分散、ユーザアカウントの保守およびリストア。処理サービスに含まれているオペレーションのセットはネットワーク管理オペレーション要求を伝えること並びにそれらを開始することおよびネットワークで選択されたノードにその結果を報告することを含んでいる。

【００２７】第１図の例によって、処理サーバ１２は、単一のホスト１６によって提供される処理サービスをホスト処理サーバ通信路２０を通じて処理するように設計

されている。しかしながら、通常の当業者は、典型的な分散形ネットワークシステムにおいて、処理サーバが数台のホストに恐らく連結されるだろうということを認証するだろう。ホスト１６は、ここに使用されているように、ネットワーク資源上で実行される一つのプロセスあるいは１セットの関連プロセスである。ネットワーク資源の例はスタンドアロンのシステム、タイムシェアリングシステム、ワークステーションおよびパーソナルコンピュータである。

【００２８】ホスト１６はホストエージェント１８によって処理サーバ１２と通信する。ホストエージェント１８および処理サーバ１２はホスト処理サーバ通信路２０を通じて通信する。一般に、ホストエージェント１８は、オペレーション要求を受信しかつ処理サービス１９によって実行されたオペレーションの結果を返すために、処理サーバ１２との通信手段を提供する。ホストエージェント１８はホスト１６の指定処理サーバ１２を認証し、管理オペレーションに指定された機能の実行を許可するホスト特定の機能性である。これらのプロセスは以下により完全に説明される。処理サービス１９は、管理オペレーション内の指定された機能を実行する。

【００２９】処理サーバ１２は、局所的なシステム２によって提供される処理サービス１９に対する要求の処理に加えて、ネットワークの他の局所的なシステムへ安全なパスで管理オペレーションを送信することおよび局所的なシステム２の機密保護を保全することに責任を負う。処理サーバ１２は管理オペレーションを転送するためにデータベース３６によって適切なリンクを決定する。データベース３６は処理サーバ間の信頼関係のリストへのアクセスを保全し制御する。信頼関係リストは、自律的なネットワークユーティリィティによる通信プロトコルの実行とは独立に生成される。これらのリストは、大域手続きによって保全されるが、管理オペレーション転送要求に対するより速い応答を提供するため、各処理サーバによって格納され、局所的にアクセス可能であるほうが好まれるだろう。二者択一的に言えば、信頼リストが局所的に格納されていないシステムにおいて、さらに応答を改善するためには、信頼関係は、現在確立されているままに局所的なシステムによって貯えられる。これらのリスト保守手順は、当業者には周知であろう。

【００３０】データベース３６によって提供されるリストは２つのカテゴリーに分割することができる。すなわち管理オペレーションの信頼された受信者および信頼された送信者である。したがって、送信処理サーバおよび受信サーバは、２つの処理サーバ間のリンク上でＲＳＭ管理オペレーションを各々伝送するためには、２つの処理サーバ間の信頼関係の存在を確認することができる。したがって、送信処理サーバは、信頼されない処理サーバへ管理オペレーションを転送しない。また、受信処理サーバは、信頼されない処理サーバによって送信された管理オペレーションを処理しない。要約すれば、データベース３６は、管理オペレーションを実行するネットワークのルートの各リンクで、処理サーバの信頼関係によって決定される安全なパスを通って、１つの処理サーバからもう一つの処理サーバまで管理オペレーションを送信するための手段を提供する。

【００３１】信頼された送受信処理サーバのリストに加えて、データベース３６は、指定されたホストに対する指定処理サーバと同様に指定された処理サービスに関連したホスト名を格納する名前空間を提供する。これによってデータベースは、管理オペレーションに指定された機能に応じて、指定処理サーバへオペレーションを転送するための信頼されたリンク情報を複数の処理サーバに提供することができる。

【００３２】第２図は、４つの（４）ネットワーク化システム（本発明の機密保護機能を使用するためのＳ１－Ｓ４）を説明するネットワーク構成を示す。各システムＳは単一の処理サーバＭおよび１つ以上のホストＣを含んでいる。特に、第２図のネットワークは階層的接続形態で配置された、Ｍ１からＭ４までの処理サーバを備えたＣ１からＣ６までのいくつかのホストシステムから成る。管理オペレーションは、Ｍ１からＭ４までの信頼された下流パスに続くことができる。しかしながら、上流へ向かう管理オペレーションを送信するための信頼されたパスは存在しない。たとえば、Ｍ２－Ｍ４はＭ１に管理オペレーションを送信することができない。さらに、この階層的接続形態ではＭ４は他の任意の処理サーバＭへ要求を転送することができない。処理サーバＭ１は、別の処理サーバＭ２への伝送と同様にホストシステムＣ１に対する処理サービスを処理する。処理サーバＭ２は、３番めの処理サーバＭ３への伝送と同様にホストＣ２およびＣ３に対する処理サービスも処理する。処理サーバＭ３は、４番めの処理サーバＭ４（それはホストＣ５およびＣ６に対する処理サービスを順番に処理する）への伝送と同様にホストシステムＣ４に対する処理サービスを処理する。

【００３３】第２図の説明のためのネットワーク接続形態に示されるように、特別の受信処理サーバへ特別の送信処理サーバからオペレーションを転送する許可は、送信者がその受信者から管理オペレーションを受信するということを必ずしも暗示しない。更に、ユーザの管理オペレーション要求を、一連の通信用にリンクされた処理サーバＭを通じて適切な処理サーバＭに送信するため、第３図の流れ図によって要約された方法の説明を容易にするための単に手段として、第２図に示されているネットワークは示されている。特定の多重システム・ネットワークの説明が本発明の範囲を制限する意図のものではないことは、通常の当業者によって認識されるだろう。

【００３４】更に、相互の信頼関係を、ネットワークの

すべての送信者および受信者のために、ネットワークプロトコルによって書取ることもできる。２つの処理サーバが相互の信頼関係を持っていて、第１処理サーバが第２処理サーバと定義された信頼関係を有し、第１処理サーバが送信者であり、第２処理サーバが受信者であっても、第１処理サーバが受信者であり、第２処理サーバが送信者である場合には、さらに信頼関係が存在しなければならない。そのような場合、信頼された送信関係および信頼された受信関係を定義するための個別のテーブルの代りに処理サーバ間の相互の信頼関係を定義する単一のテーブルを保全することだけが必要である。

【００３５】本発明によってＲＳＭオペレーションに提供されるリンク状の機密保護手段について詳細に説明するために、第２図のネットワーク構成に関連して第３図に説明された方法を参照しながら、ホストＣ４によって処理され、Ｍ１のユーザー・インターフェースで実行依頼された処理サービスによって実行されるＲＳＭ機能を実行するためのプロセスを説明することにする。指定されたＲＳＭ機能の実行は、ユーザ処理サーバインタフェースに認証されたユーザによる管理オペレーションの実行依頼でステップ１００から始まる。前に説明したように、協力する処理サーバによってディスパッチされかつホスト上で指定された処理サービスによって実行される特定の機能について、管理オペレーションは説明する。

【００３６】管理オペレーションの受信後、処理サーバＭ１は“転送”手続１０１を始める。リンクに対するすべての管理オペレーションを伝送中送受信管理オペレーションによって実行される２つのタスク、すなわち
（１）相互の確認、および、（２）処理サーバ間の信頼によって、転送手続きの間安全なパスの保全が促進される。

【００３７】処理サーバＭ１は、管理オペレーションがユーザ処理サーバインタフェースから最初に受信される発信地であり、“発信処理サーバ”と呼ばれる。“指定処理サーバ”は指定された処理サービスのためのホストを管理する処理サーバである。以前に言及したように、“処理サービス”とは、指定された管理オペレーションとして指定された機能を実行する１セットの関連するプロセスである。

【００３８】転送手続き１０１のステップ１０２で、発信処理サーバＭ１は、それがデータベース３６による管理オペレーションのための指定処理サーバであるかどうかを決める。発信処理サーバがさらに指定処理サーバならば、コントロールはステップ１１４に移り、転送ループ１０３は迂回される。しかしながら、その後、もし発信処理サーバが指定処理サーバでなければ、ステップ１０４へコントロールが移る。本例においては、処理サーバＭ１が指定処理サーバでないので、コントロールは、転送手続き１０１のステップ１０４に移る。

【００３９】ステップ１０４で、次のオブジェクト？への管理オペレーションの転送に現在責任を負う処理サーバ、今の場合、発信サーバＭ１は、処理サーバＭ１によって管理されたホストかあるいは別の処理サーバである適切なオブジェクト？へ管理オペレーションを転送するために、データベース３６および指定処理サーバ（Ｍ３）の身元確認によって保全された、オブジェクト間の信頼関係に基いてルーティング情報を得る。ステップ１０５で、処理サーバＭ１は、指定処理サーバへの信頼されたパス上に管理オペレーションを受信するための信頼された処理サーバが存在するかどうかを決めるために、データベース３６に問い合わせる。もし信頼された受信処理サーバが存在しなければ、転送手続き１０１が異常終了させられる。しかしながら、もし信頼された受信者が存在すれば、データベース３６は、管理オペレーションのための信頼された受信者の身元を返す。その後、コントロールはステップ１０６に移る。

【００４０】本例において、処理サーバＭ２は、Ｍ１からＣ４までの“信頼された”パス上で管理オペレーションを中継するための適切な手段を提供する。すなわちコントロールはステップ１０６に移り、そこで、処理サーバＭ１、Ｍ２は、キーベースの“Kerbesos”確認サービスのようないくつかの有名な受信可能手段の１つによって相互の認証を実行する。無許可のパーティは、認証中は処理サーバＭ１、Ｍ２の間で送信されるメッセージを単にモニタすることによっては、正当なユーザのキーを割り当てることができないので、システム設計者は暗号に基いた確認スキームのほうを好んで選択してもよい。他の適切な確認メカニズムも通常の当業者に知られているだろう。処理サーバＭ１、Ｍ２よって認証が試みられた後、コントロールはステップ１０７に移り、ここで、処理サーバＭ１、Ｍ２は、相互の認証が成功裡に生じたかどうかを別個に決める。相互の認証が失敗の場合、転送手続き１０１は、意図された送信者あるいは受信者のいずれかによって異常終了させられる。しかしながら、その後、送信Ｍ１処理サーバおよび受信Ｍ２処理サーバが互いの身元を相互に認証すれば、コントロールはステップ１０８へ移る。

【００４１】データベース３６は、各受信処理サーバのために信頼された送信処理サーバに関する情報を提供する。受信処理サーバは、データベース３６によって保全されている信頼関係にしたがって信頼された送信処理サーバからの管理オペレーションを受信するだけである。ステップ１０８で、処理サーバＭ２は発信処理サーバＭ１が管理オペレーションの信頼された送信者かどうかを決めるために、データベース３６に問い合わせる。送信者および受信者管理オペレーションを相互に確認するための前述の方法は、典型的なものである。相互の信頼の存在を確認する他の方法は、当業者に知られているであろう。処理サーバＭ２が送信処理サーバＭ１を信頼しないということをデータベース３６が受信処理サーバＭ２

に通知した場合、受信処理サーバM２は転送手続き１０１を異常終了させる。しかしながら、その後受信処理サーバM２が送信処理サーバM１を信頼した場合、ステップ１１０へコントロールが移る。

【００４２】処理サーバM１とM２が、互いを認証し、信頼関係が２つのサーバ間に存在することを確認した後、ステップ１１０で処理サーバM１は、第２図に図解されているように通信リンク４４を通じて処理サーバM２へ管理オペレーションを転送する。管理オペレーションが、指定処理サーバに達する前に、いくつかの処理サーバMを通りぬけることもあるので、ステップ１１２で、受信者M２がそれが管理オペレーションで身元確認された機能に対する指定の管理オペレーションであるかどうかを決めることが必要である。受信処理サーバM２が指定処理サーバではない場合、コントロールは転送ループ１０３のステップ１１２まで移り、処理サーバM２は、指定処理サーバへの信頼されたパス上の次の受信処理サーバを決定するために、データベース３６に問い合わせる。本例では、通信リンク４６を介して処理サーバM３へ管理オペレーションを転送する前に、送信処理サーバM２と受信処理サーバM３は互いを認証し、処理サーバM２とM３の間の相互の信頼関係の存在を確認して、転送プロセスが継続する。

【００４３】指定処理サーバM３がステップ１１０で管理オペレーションを受信した後、コントロールは、転送ループ１０３のステップ１１２に移る。処理サーバM３は、それが管理オペレーションに記述された機能を実行するように指定された処理サービスのためのホストC４に対する指定処理サーバであることを決める。その後、コントロールは転送ループ１０３からステップ１１４に移る。もし指定のホストがC４ではなく、C５あるいはC６だったならば、処理サーバM３およびM４は、通信リンク４８を介して、M４へ管理オペレーションを転送するために転送手続き１０１の範囲内で、転送ループ１０３の補足反復を実行するために協力するだろう。

【００４４】転送手続きの確認ステップ１０６は、電話回線のような物理的に露出された伝送リンク上で送信された情報を保護するための手段を提供する。この特徴は処理サーバ間の伝送リンクが盗聴器から物理的に守られない特別の例における利点を提供するけれども、当業者によって認識されているように、認証というものはすべての例において必ずしも必要な要素ではない。

【００４５】指定のホストC４に管理オペレーションを転送することができる前に、ホストC４および処理サーバM３は互いを認証し、相互の信頼関係がサーバとホスト間に存在することを確認する。この手続きは、第３図の図解で示されている方法でステップ１１４において実行される。その後、コントロールは１１６へ移り、そこで、もしユーザが管理オペレーションに指定された機能の実行を要請することが許可されれば、処理サービスによるホストC４が管理オペレーションによって指定された機能を実行する。

【００４６】ホスト１６によって実行された各管理オペレーションに対して、ホストエージェント１８としてここで言及されているプロセスは、処理サービスが要求された機能を実行することを認める前に、オペレーションを実行依頼したユーザの許可をチェックする。許可データは、各ホスト１６のための局所的なデータベースに含まれており、このデータベースには、ユーザおよび（複数の部類の）オペレーションのリスト、および（若しくは）、各ユーザが許可されている複数のセットの特権が保全されている。各ホスト１６に対する許可データベース（別個に図解されてはいない）は、ホスト１６の局所的アドレススペース内に典型的に保全されている。ホスト１６の局所的アドレススペース内にユーザ許可情報を保全することによって、ホスト１６は、許可データの保全性の保護に対する最終的な決定権を有している。そのデータをほかの場所に格納することは、無許可のプロセスによって変更される危険性にそれをさらすことになる。

【００４７】処理オペレーションの実行は、１つ以上の処理サーバMによって役立てられる複数のホストCを含んでいてもよい。例えば、ホストC１に最初に実行依頼される管理オペレーションを考えなさい。そのホストC１は、要求に応じて、第２の管理オペレーションを実行依頼し、この第２の管理オペレーションは、以下、ホストC４に対して“コマンド”と呼ばれることになろう。第２のホストC４にコマンドの実行を依頼するホストC１に対する処理サーバM１は、第３図に関連して説明した前述の相互の認証および信頼関係手続きにしがって、そのコマンドを転送する。第２のホストC４はコマンドを受信すると、このコマンドが許可されたかどうかを決めるためにその指定処理サーバM３でチェックしなければならない。ホストC４は、第３図に図解され、また、認証されたユーザによってホストCに直接実行依頼された管理オペレーションに関連して、以前に説明された、手続きのステップ１１４での認証および許可手続きによって許可を確認する。したがって、第２のホストC４は、コマンドが、ネットワークリンクによる信頼されたパスを通って許可されたユーザによって実行依頼され、許可された管理オペレーションから発信したことをホストC４が確定した後でのみ、コマンドによって記述された機能を実行する。機密保護がリンク上の基礎の上に確立されるので、コマンドがその信頼された処理サーバM３によってホストC４により受信されたことを確認することによって、信頼されたパスは、単に推論されるだけである。さらに、ネットワーク伝送の機密保護は第２のホストC４に対して処理サーバM３に、ホストC４がそのコマンドを実行するようにホストC１が実行依頼したことを確認するために、実行依頼するホストC１に対し

て処理サーバM１に問い合わさせることによって増強される。

【００４８】したがって、ここに、データブロックの送信者と受信者間の相互の信頼の関係を確立するための手段を提供することによって、許可された個人だけが特定のシステム上で特定の管理オペレーションを実行したり受信することが許可されることを保証する機密保護機能を提供する方法が説明された。追加の請求の範囲で述べられるような本発明の原理及び範囲外に危険を冒して進むことなく、詳細な諸点における変更およびここに説明されたプロセスの配置の変更を当業者が行なってもよいことは理解されるであろう。

【図面の簡単な説明】

この発明のより詳細な理解は、付属図面と関連して読むことにより、典型的な推奨実施例の次の説明から得られるであろう。

【図１】本発明を具体化する適切な分散形ネットワークシステムのブロック図である。

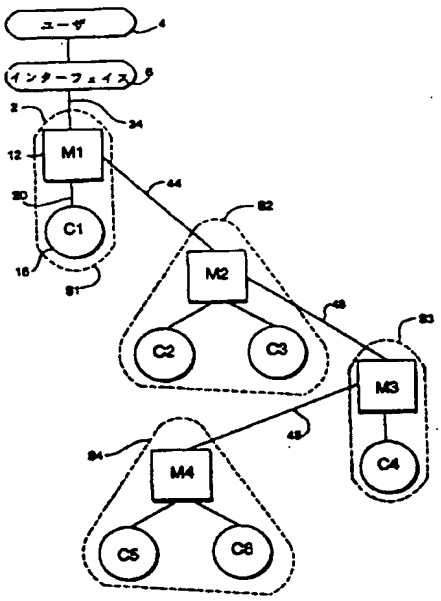
【図２】本発明の教えを使用する分散形ネットワークシステムにおける、いくつかの処理サーバおよびホストの説明のための図式表現である。

【図３】本発明に従って、オペレーションの実行を転送しその後実行するために使用されるステップの説明のための流れ図である。

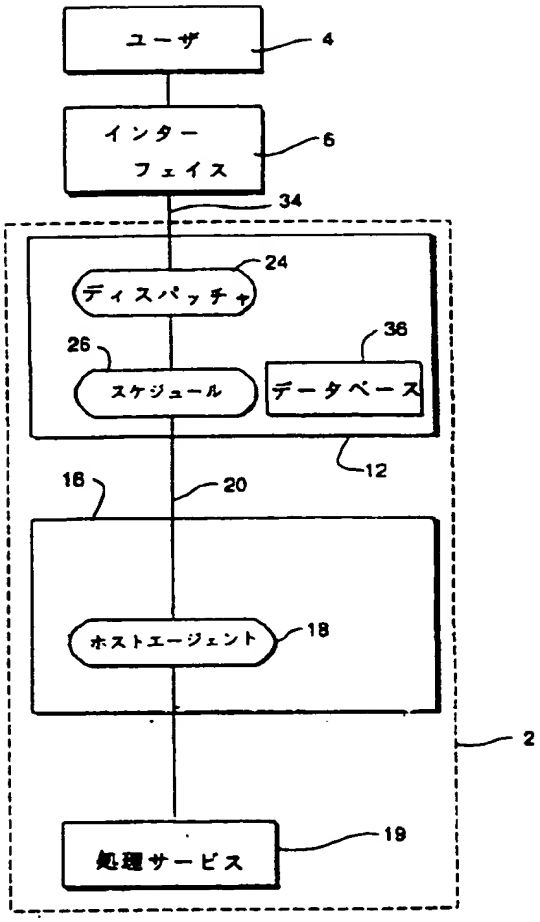
【符号の説明】

４　ユーザ
６　インターフェース
１２　データベース
１８　ホストエージェント
１９　処理サービス
２４　ディスパッチャ
２６　スケジュラ
３６　データベース

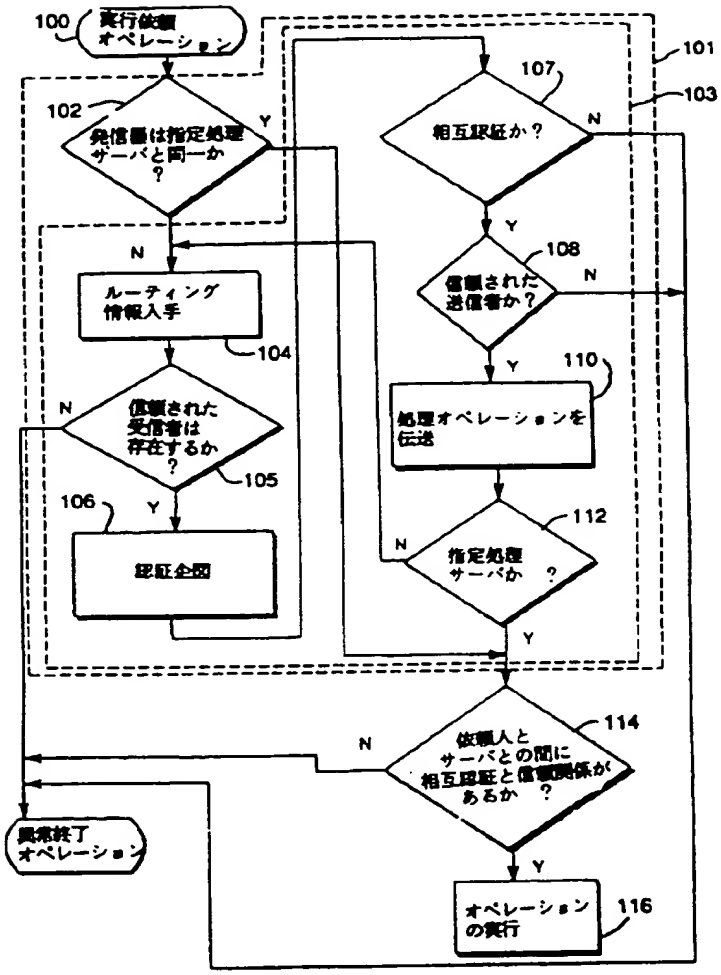
【図２】



【図１】


ユーザ
4
インター
フェイス
6
34
24
ディスパッチャ
26
スケジュール
36
データベース
12
16
20
ホストエージェント
18
2
処理サービス
19

【図3】



フロントページの続き

(72)発明者　デヴィッド　マイケル　グリフィン
アメリカ合衆国　マサチューセッツ州　01754メイナード　サマーヒル　ロード　52
(72)発明者　ブラッド　シー　ジョンソン
アメリカ合衆国　ロード　アイランド州　02891ウェスターリィ　オーク　ストリート　45
(72)発明者　ディクター　シィリー
アメリカ合衆国　マサチューセッツ州　02118ボストン　コロンバス　アヴェニュー　650
(72)発明者　ジェームズ　シェルハマー
アメリカ合衆国　マサチューセッツ州　01754メイナード　コンコード　ストリート　26

(72)発明者　オーウェン　ハロルド　トールマン
アメリカ合衆国　マサチューセッツ州
01462ルーネンバーグ　マサチューセッツ
アベニュー　852